Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

Advanced QKD Protocols and Practical Challenges

Mohit Rajpurohit, Kaustubh Moni Deka, Vaibhav Pratap Singh, Haribabu P

Centre for Development of Advanced Computing - Bengaluru

C-DAC

https://pkiindia.in

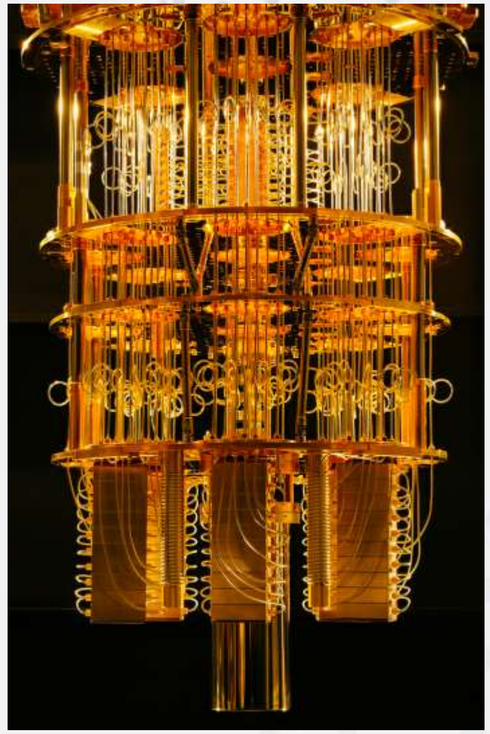
Social Media /pkiindia

IEEE BANGALORE SECTION

Outline

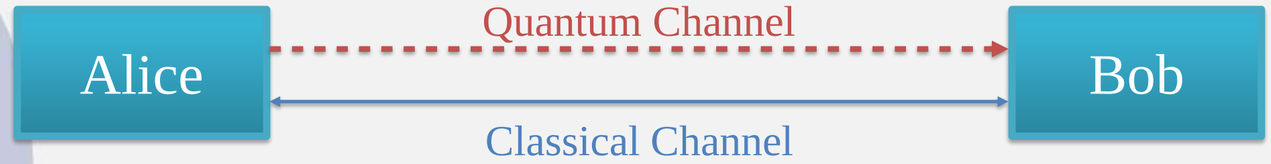
- ✦ Motivation
- ✦ Quantum Cryptography
- ✦ Advanced Quantum Key Distribution (QKD)
- ✦ Measurement Device Independent - QKD
- ✦ Twin Field - QKD
- ✦ Quantum Hacking
- ✦ Quantum Random Number Generator (QRNG) Integration
- ✦ Control Electronic Architecture
- ✦ Practical Challenges in Field Implementation

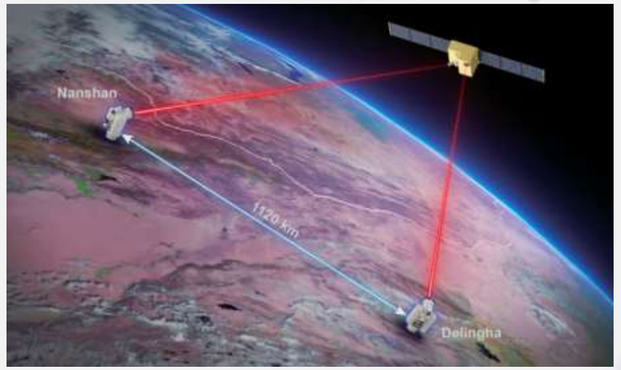
Prof. Richard Feynman

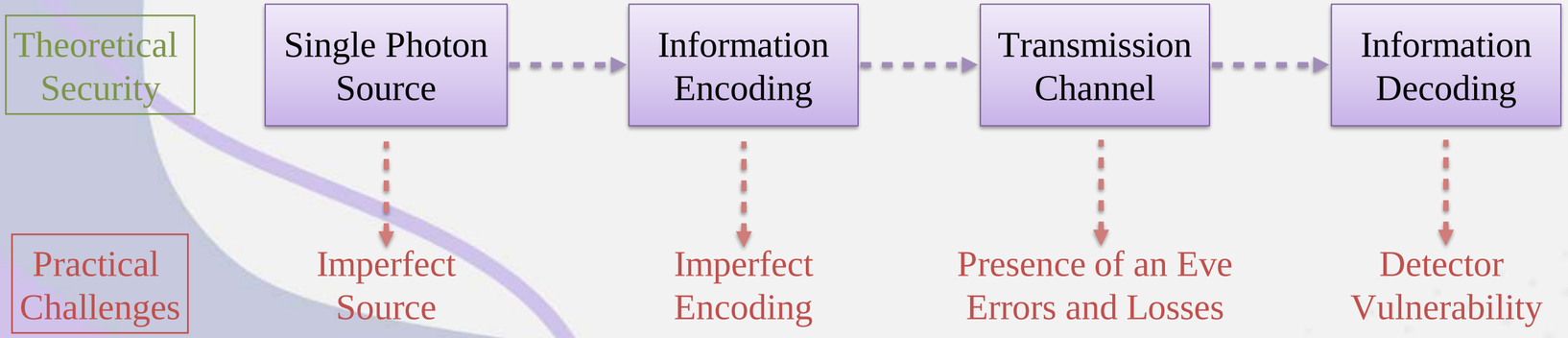


Quantum Cryptography

✦ Quantum Key Distribution (QKD) is a secure **Symmetric key** distribution technique whose **Unconditional Theoretical Security** is assured by the **laws of Quantum Mechanics**.







Measurement Device Independent - QKD

✦ It removes the Dependency from the Measurement Devices (Single Photon Detector)

Protocol

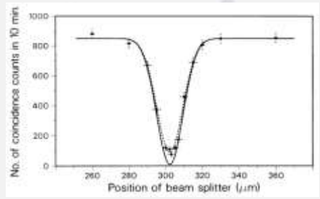
- **State Preparation:** Alice and Bob individually prepare a **phase randomized** weak coherent pulses(WCP) $|\sqrt{\mu_a}e^{i\theta_a}\rangle$ and $|\sqrt{\mu_b}e^{i\theta_b}\rangle$ with few different decoy intensities $\mu_a\ \mu_b \in [\mu, \nu, 0]$.
- **Measurements:** Alice and Bob send their quantum state to the **untrusted** third party **Charlie** to perform the **two photon interference** measurement on their state.

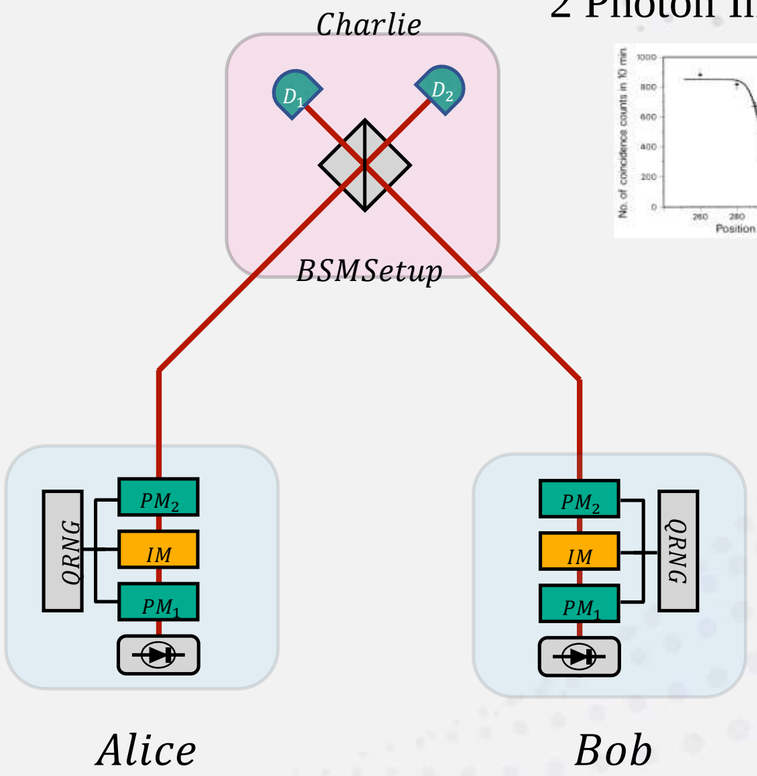
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]$$

Advantages

✦ Immune to all possible Detector based attacks
✦ A Star Type Network Topology
✦Sustain with High Channel Loss
✦ Untrusted Nodes
✦ Practicality

2 Photon Interference

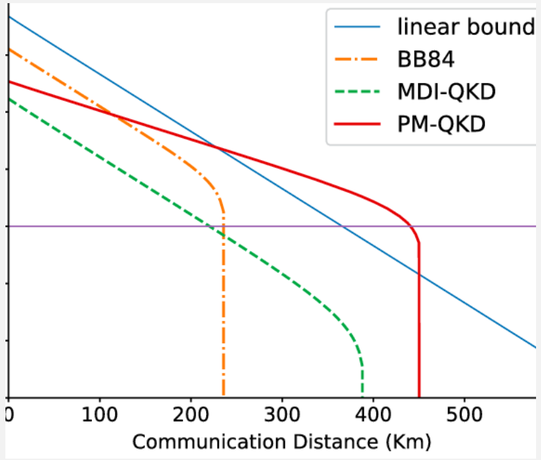


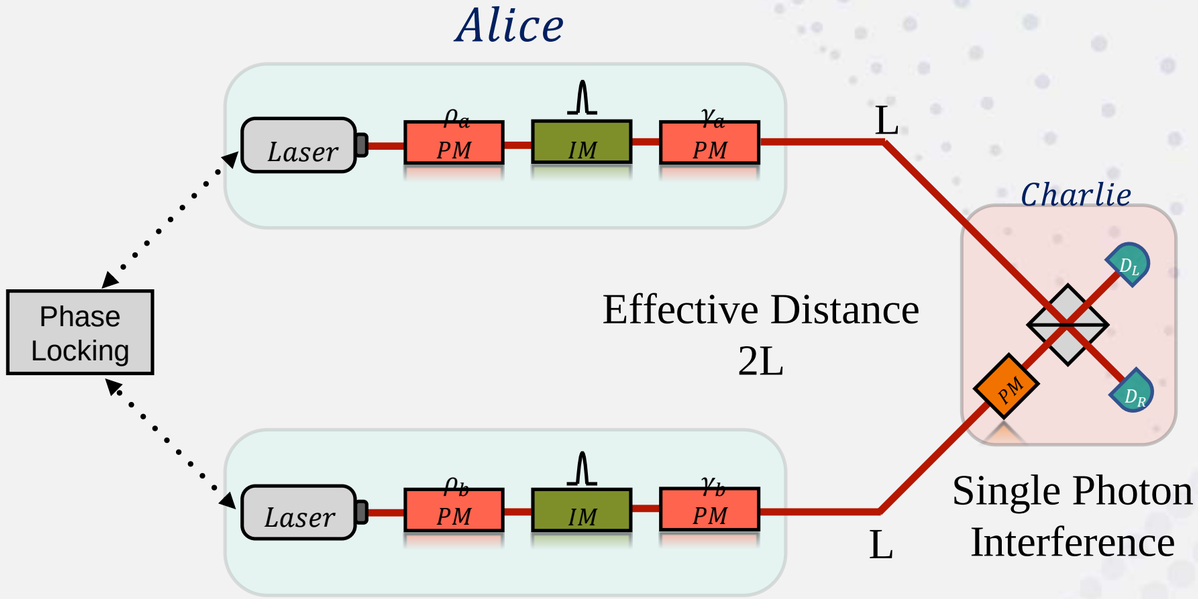


Twin Field - QKD

- The secret key capacity of a quantum channel sets an **upper bound** on the maximum extractable secret key, given by the **PLOB** bound…

$$R_{PLOB} = -\log_2(1-\eta)$$





Protocol

- **State Preparation:** Alice and Bob prepare a **Twin** like **Quantum Optical Modes**.
- **Measurements:** Alice and Bob send their optical modes to the central **relay station** Charlie. At the central, Charlie observes the **Single Photon Interference**.

Advantages

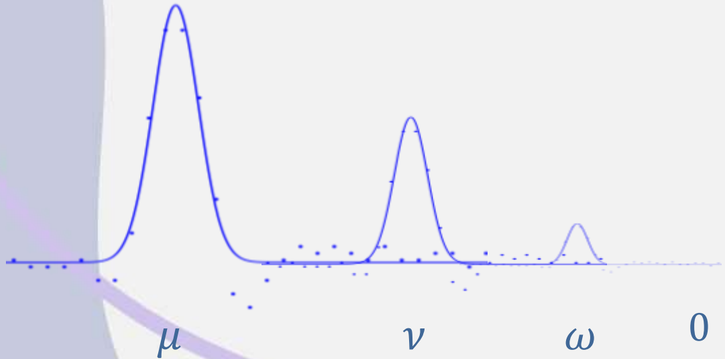
- All the MDI-QKD Features
- SKR $R \sim O(\sqrt{\eta})$

Quantum Hacking

- A **Weak Coherent State** can be described by a Mixture of **Fock states**.

$$|\alpha\rangle = e^{-\frac{|\mu|^2}{2}} \sum_{n=0}^{\infty} \frac{\mu^n}{\sqrt{n!}} |n\rangle$$

- By **Measuring** and **Monitoring** the **Parameters** of the QKD system, the **Leaked Information** can be estimated.



Decoy Intensities

- The **Imperfection** of the Practical devices leaves potential **Loopholes** for Eve to **SPY** the **Final Secret Key**.

Eavesdropper Strategy

Unambiguous State Discrimination (USD) Attack

POVM Measurement

+

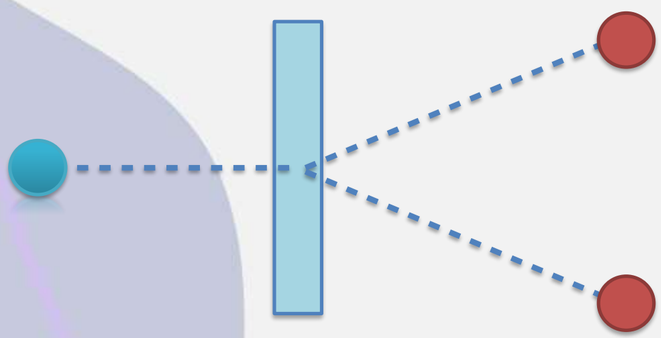
Photon Number Splitting (PNS) Attack

Multi Photon Emission

Solution

Phase Randomization Of Weak Coherent Source

Quantum Random Number Generator Integration



Heralded Single Photon Source

Beam Splitter

Bit 0

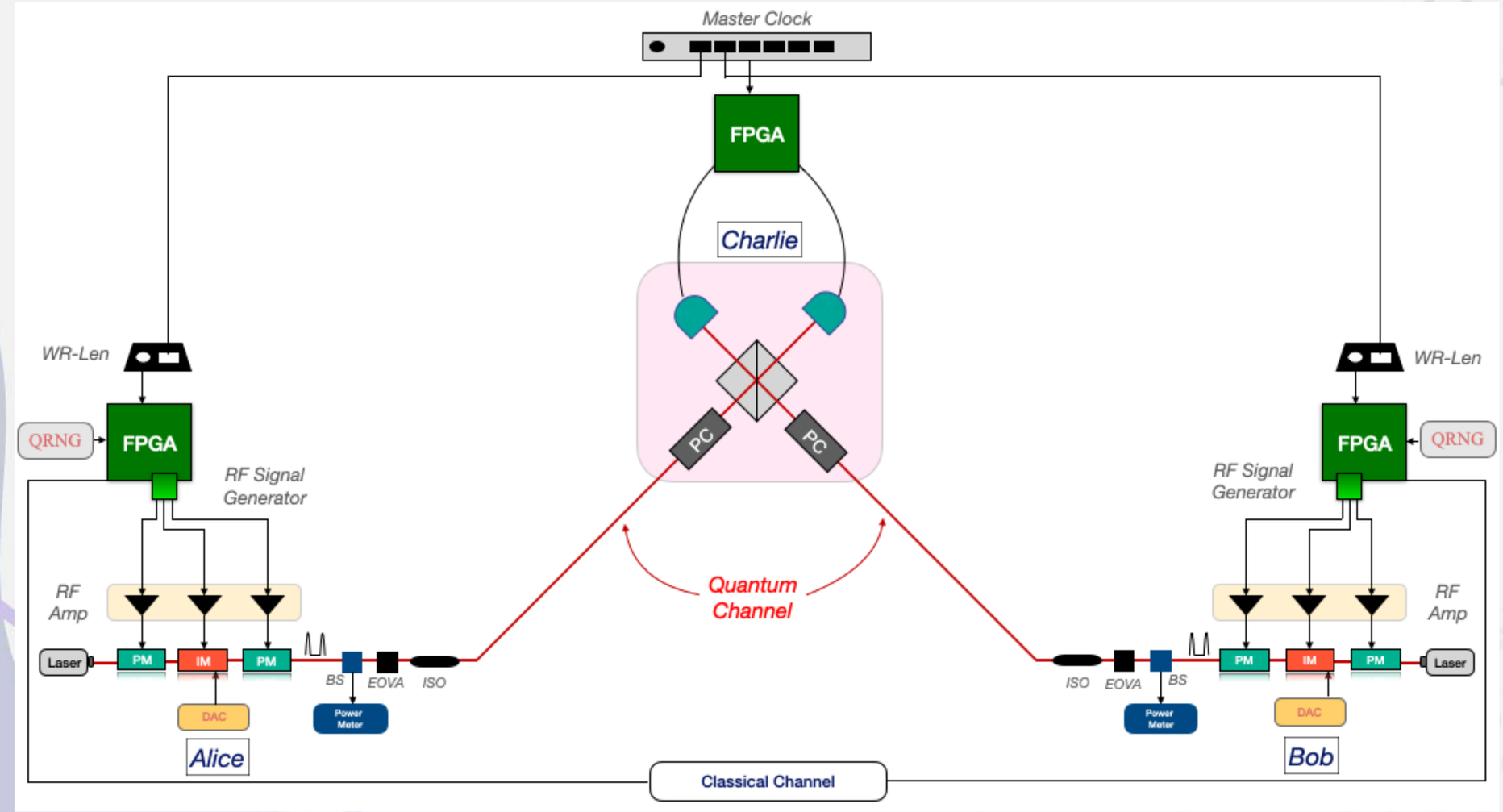
Bit 1

NIST Randomness Test

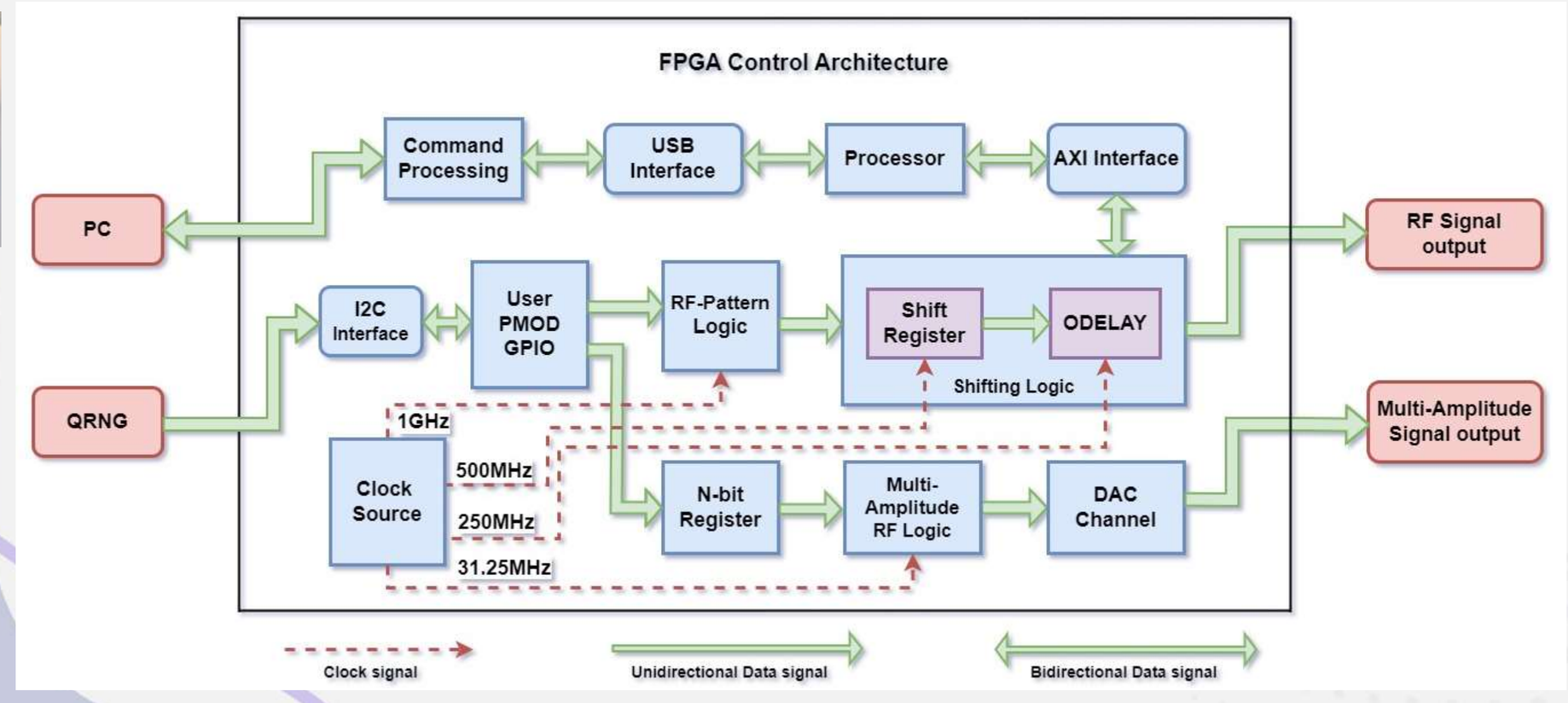
…	…	1	0	0	1	0	1	1

Random Bit String

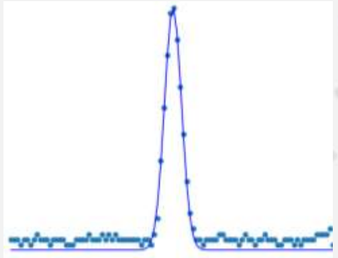
MDI-QKD Setup



FPGA Based Control Electronics



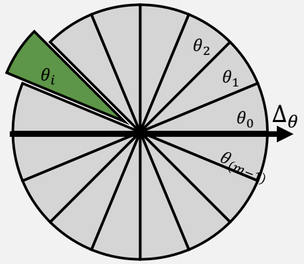
RF Signal



1 GHz Signal
Fine 4 ps Shifting

Experimental Results

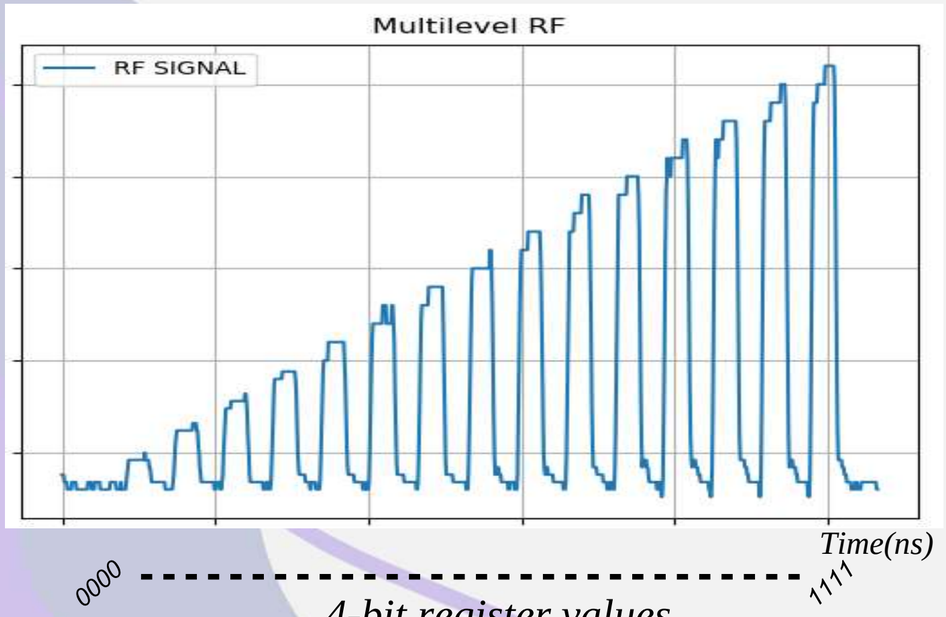
Discrete Phase Randomization

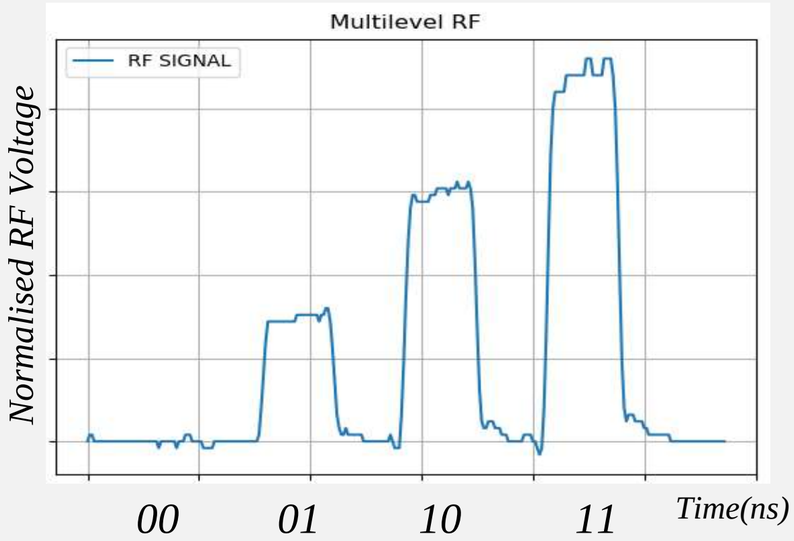


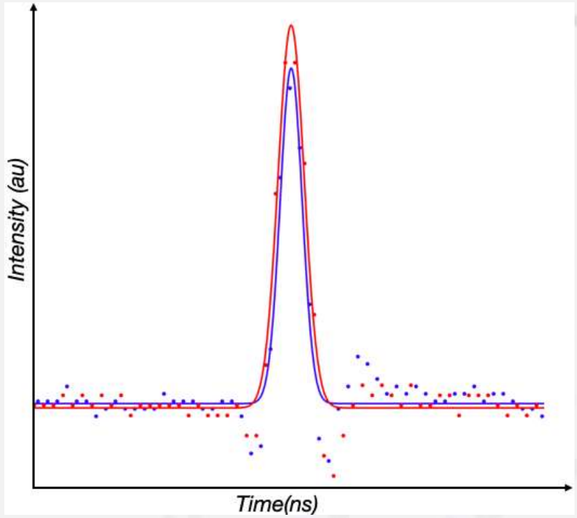
Phase Encoding

$$\left\{ 0 \quad \frac{\pi}{2} \quad \pi \quad \frac{3\pi}{2} \right\}$$

Phase Randomized Optical Signal







1 GHz Optical Signal

Devetek-Winter Bound

$$SKR \geq \frac{2}{M} Q_\mu [1 - H_2(e_p) - f H_2(e_\mu)]$$

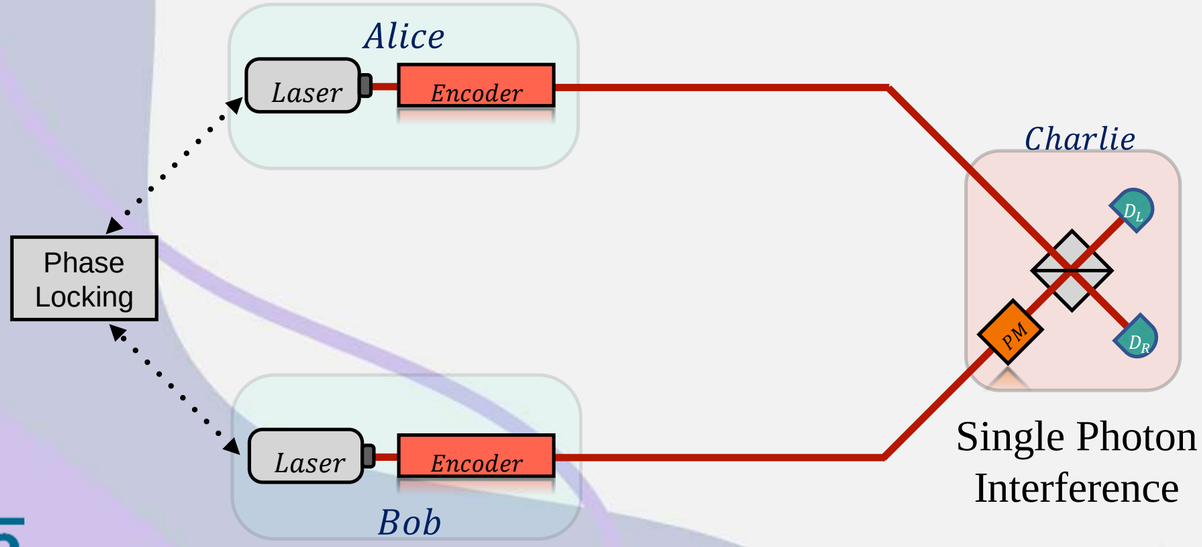
Practical Challenges in Field Implementation

Photon Interference

- Perfect **Temporal Overlapping**
- **Polarization** need to be Identical
- **Phase** of an Optical Signals need to be Correlated

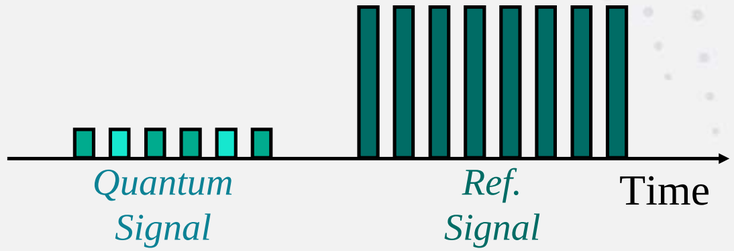
Phase Evolution

A. Phase of an **Optical Source**
B. Phase Introduced by **Optical Channel**



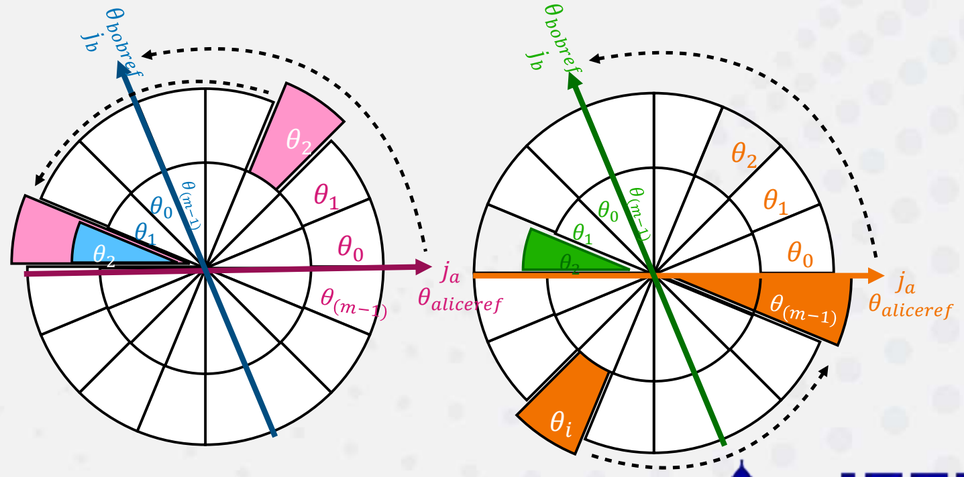
Single Photon Interference

1. No Phase Post Selection (NPP) Protocol



Time Multiplexed Signal

2. Phase Post Selection (NPP) Protocol



Conclusion

- **Experimentally** Generated a **Phase Randomised Optical Signal (Initial Quantum State)** using **Weak Coherent Sources** and **Electro Optical Modulators**
- Developed a **Control Electronics Hardware Design** based on **FPFG.**
- Detailed analysis of **practical challenges** for **field implementation**.

References

- H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012
- Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement- device-independent quantum key distribution over untrustful metropoli- tan network," *Physical Review X*, vol. 6, Mar. 2016
- S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, Apr. 2017.
- M.Lucamarini,Z.L.Yuan,J.F.Dynes,andA.J.Shields,"Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.
- Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New Journal of Physics*, vol. 17, p. 053014, May 2015.
- C.-M. Zhang, Y.-W. Xu, R. Wang, and Q. Wang, "Twin-field quantum key distribution with discrete-phase-randomized sources," *Phys. Rev. Appl.*, vol. 14, p. 064070, Dec 2020.
- H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, Jun 2005.
- Y. Mao, P. Zeng, and T. Chen, "Recent advances on quantum key distribution overcoming the linear secret key capacity bound," *Advanced Quantum Technologies*, vol. 4, Nov. 2020
- Guide, "Advance specification user guide for xilinx zynq ultrascale+ processor architecture clocking resources," 2013.
- Xilinx, "Advance specification user guide for xilinx zynq ultrascale+ rfsoc rf data converter v2.4 gen 1/2/3 product guide," 2020.

THANK YOU